

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

A. KAWAMOTO

3/14/01

63597

10fl



別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日  
Date of Application:

2000年 3月15日

出 願 番 号  
Application Number:

特願2000-073064

出 願 人  
Applicant(s):

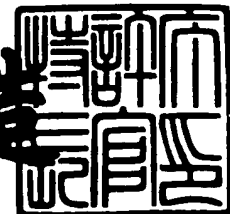
日本電気株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 1月26日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



出証番号 出証特2001-3001749

【書類名】 特許願

【整理番号】 37400189

【提出日】 平成12年 3月15日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 13/00

【発明の名称】 マルチキャストシステム、認証サーバ端末、マルチキャスト受信者端末管理方法、並びに記録媒体

【請求項の数】 9

【発明者】

    【住所又は居所】 東京都港区芝五丁目7番1号 日本電気株式会社内

    【氏名】 川本 亜紀子

【特許出願人】

    【識別番号】 000004237

    【氏名又は名称】 日本電気株式会社

【代理人】

    【識別番号】 100108578

    【弁理士】

    【氏名又は名称】 高橋 詔男

【代理人】

    【識別番号】 100064908

    【弁理士】

    【氏名又は名称】 志賀 正武

【選任した代理人】

    【識別番号】 100101465

    【弁理士】

    【氏名又は名称】 青山 正和

【選任した代理人】

    【識別番号】 100108453

    【弁理士】

【氏名又は名称】 村山 靖彦

【手数料の表示】

【予納台帳番号】 008707

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9709418

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 マルチキャストシステム、認証サーバ端末、マルチキャスト受信者端末管理方法、並びに記録媒体

【特許請求の範囲】

【請求項 1】 マルチキャストにおける送信者端末と受信者端末の管理を行う認証サーバ処理装置と、

該認証サーバ処理装置に対するログインを行う第 1 のユーザ処理装置を有し、マルチキャストデータを送信する送信者端末と、

該認証サーバ処理装置に対するログインを行う第 2 のユーザ処理装置を有し、マルチキャストデータを受信する受信者端末と、

を備えるマルチキャストシステム。

【請求項 2】 前記送信者端末はマルチキャストデータを送信する際に、第 1 のユーザ処理装置から前記認証サーバ処理装置に対してログイン要求を行い、前記認証サーバ処理装置からログインを許可されると、マルチキャストデータを暗号化して送信することを特徴とする請求項 1 に記載のマルチキャストシステム。

【請求項 3】 前記受信者端末は予め前記認証サーバ処理装置に登録されており、マルチキャストデータを受信する際に、第 2 のユーザ処理装置から前記認証サーバ処理装置に対してログイン要求を行い、前記認証サーバ処理装置からログインを許可されると、前記認証サーバ処理装置から渡された暗号鍵を用いてマルチキャストデータを復号化してアプリケーションを受信することを特徴とする請求項 1 に記載のマルチキャストシステム。

【請求項 4】 前記認証サーバ処理装置に登録していない前記受信者端末はマルチキャストデータを受信する際に、第 2 のユーザ処理装置から前記認証サーバ処理装置に対してログイン要求を行うが、前記認証サーバ処理装置からログイン不許可となり暗号鍵は渡されないことを特徴とする請求項 1 に記載のマルチキャストシステム。

【請求項 5】 前記認証サーバ処理装置は定期的に暗号鍵を生成し、ログイン時と同様に暗号鍵を受信者端末へ配布し、定期的に配布する暗号鍵を該受信者

端末のユーザ処理装置が受け取らなかった場合は、前記認証サーバ処理装置にてログアウト処理を行うことを特徴とする請求項 1 又は請求項 3 に記載のマルチキャストシステム。

【請求項 6】 前記受信者端末のアプリケーションでマルチキャスト通信を終了すると、該受信者端末のユーザ処理装置が前記認証サーバ処理装置に対してログアウト要求を行い、前記認証サーバ処理装置は該当ユーザの管理を終了することを特徴とする請求項 1、請求項 3 又は請求項 5 に記載のマルチキャストシステム。

【請求項 7】 マルチキャストデータを送信する送信者端末に設けられた第 1 のユーザ処理装置からのログイン要求を受理する手段と、

マルチキャストデータを受信する送信者端末に設けられた第 2 のユーザ処理装置からのログイン要求を受理する手段と、

送信者端末を有するユーザの個人情報が登録されたユーザ登録情報手段と、  
を備える認証サーバ端末であって、

前記認証サーバ処理装置からログインを許可された送信者端末はマルチキャストデータを暗号化して送信し、

前記認証サーバ処理装置から予めユーザ登録情報手段にユーザとして登録された受信者端末は、ログインを許可されると共にマルチキャストデータを受信することを特徴とする認証サーバ端末。

【請求項 8】 送信者端末を有するユーザの個人情報を登録し、

マルチキャストデータを送信する送信者端末からのログイン要求を受理し、

ログインを許可された送信者端末はマルチキャストデータを暗号化して送信し

マルチキャストデータを受信する送信者端末からのログイン要求を受理し、

前記認証サーバ処理装置から予めユーザ登録情報手段にユーザとして登録された受信者端末は、ログインを許可されると共にマルチキャストデータを受信することを特徴とするマルチキャスト受信者端末管理方法。

【請求項 9】 送信者端末を有するユーザの個人情報を登録するステップと

マルチキャストデータを送信する送信者端末からのログイン要求を受理するステップと、

ログインを許可された送信者端末はマルチキャストデータを暗号化して送信するステップと、

マルチキャストデータを受信する送信者端末からのログイン要求を受理するステップと、

前記認証サーバ処理装置から予めユーザ登録情報手段にユーザとして登録された受信者端末は、ログインを許可されると共にマルチキャストデータを受信するステップと、

を有するマルチキャスト受信者端末管理方法のプログラムがコンピュータの利用可能な状態で記録された記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、マルチキャストによるデータ通信に関し、特に指定された認証サーバで参加者を個別認証することにより参加者を特定する構成に関する。

【 0 0 0 2 】

【従来の技術】

マルチキャストは、ユニキャストとブロードキャストの概念を総合したものである。つまり、マルチキャストデータが特定のホストに送られたり（ユニキャスト）、ネットワーク上の全ホストに送られる（ブロードキャスト）のではなく、任意の数のホストにデータパケットが同時に送られる。送信者はマルチキャストグループアドレスにデータを送り、そのデータの受信を希望する者は誰でも受信可能であることは既知である。また、暗号化を使用するデータストリーム保護方法は公知であり、送信者が受信者側での解読のためにデータパケットを暗号化するものである。

【 0 0 0 3 】

これは一般的に共通鍵暗号化技術を使用する。従来のマルチキャストにおけるデータフロー保護技術の一例が、特開平11-027252号公報と特開平11-127197号公

報に記載されている。特開平11-027252号公報では、鍵の扱いとして、データの暗号／復号に使用する鍵（公開鍵／秘密鍵）を鍵管理装置に保管する構成になっていると共に、マルチキャスト技術は復号鍵の配布に利用する構成が開示されている。特開平11-127197号公報では、鍵の扱いとしてユーザ認証に使用する鍵（共用キー／専用キー）はすべてドメインネームサーバまたは認証機関に保管する構成になっている。

また、特開平11-127197号公報に記載されている従来のマルチキャストにおけるデータフロー保護技術は、ユーザがマルチキャストに参加要求を出すとマルチキャストルータがドメインネームサーバにインストールされた共用キーを検索し、ユーザが認証されるべきか否かを判断するルーティングエレメント制御である。これによって認証されないユーザのアクセスは遮断される。

#### 【 0 0 0 4 】

##### 【発明が解決しようとする課題】

しかし、特開平11-027252号公報記載の技術では、復号鍵を取得可能なユーザは不特定多数であり、復号鍵を持っていれば解除時刻後に暗号化データを解読することが可能であるという問題点があった。また、特開平11-027252号公報の技術では、暗号鍵を取得可能なユーザは送信を許可されたユーザのみで、危険なデータの送出を避けることができるが、復号鍵の取得が可能なユーザはルータ以下の不特定多数であり、復号鍵を持っていれば暗号化データを解読することが可能である。即ち、認証サーバに登録されたユーザでなくともマルチキャストデータ送受信可能になるという課題があった。

#### 【 0 0 0 5 】

さらに、マルチキャスト通信において、現在誰がマルチキャストデータを送受信しているのかわからず、ユーザ別の対応ができないという問題点がある。その理由は、ネットワーク上のホストはIGMP (Internet Group Management Protocol) を使ってグループメンバーシップ情報をローカルマルチキャストルータに知らせるが、その知らせを受けたマルチキャストルータはローカルマシンに必要なパケットだけ転送する。マルチキャストルータは、自分のサブネットにどのホスト・グループのパケットを流せばよいのかわかればよいので、実際に誰が参加し

ているのか、また何人参加しているかは、管理者も参加者の誰にも知らされない。別の問題点は、重要なマルチキャストデータを盗まれたことに気づかないことである。参加者を確定できれば、マルチキャスト通信による放送・会議でユーザごとのメンテナンスが可能になる。

本発明は上述する課題を解決するもので、マルチキャストによるデータ通信において、指定された認証サーバで参加者を個別認証することにより参加者を特定できるマルチキャストシステムを提供することを目的とする。

#### 【 0 0 0 6 】

##### 【課題を解決するための手段】

上記課題を解決する本発明のマルチキャストシステムは、図 1 に示すように、マルチキャストにおける送信者端末 1 1 0 と受信者端末 1 3 0、1 4 0 の管理を行う認証サーバ処理装置 1 0 1 と、該認証サーバ処理装置に対するログインを行う第 1 のユーザ処理装置 1 1 2 を有し、マルチキャストデータを送信する送信者端末 1 1 0 と、該認証サーバ処理装置に対するログインを行う第 2 のユーザ処理装置 1 3 2 を有し、マルチキャストデータを受信する受信者端末 1 3 0 とを備えるものである。

#### 【 0 0 0 7 】

好ましくは、送信者端末 1 1 0 はマルチキャストデータを送信する際に、ユーザ処理装置 1 1 2 から認証サーバ処理装置 1 0 1 に対してログイン要求を行い、認証サーバ処理装置 1 0 1 からログインを許可されると、マルチキャストデータを暗号化して送信する構成とするとよい。

#### 【 0 0 0 8 】

また、受信者端末 1 3 0 のユーザは、認証サーバ処理装置 1 0 1 に登録されているユーザとする。受信者端末 1 3 0 はマルチキャストデータを受信する際に、ユーザ処理装置 1 3 2 から認証サーバ処理装置 1 0 1 に対してログイン要求を行い、認証サーバ処理装置 1 0 1 からログインを許可されると、認証サーバ処理装置 1 0 1 から渡された暗号鍵を用いてマルチキャストデータを復号化してアプリケーション 1 3 1 で正常に受信することができる。

#### 【 0 0 0 9 】



また、受信者端末 1 4 0 のユーザは、認証サーバ処理装置 1 0 1 に登録されていないユーザとする。受信者端末 1 4 0 はマルチキャストデータを受信する際に、ユーザ処理装置 1 4 2 から認証サーバ処理装置 1 0 1 に対してログイン要求を行うが、登録されていないので認証サーバ処理装置 1 0 1 からログイン不許可となり暗号鍵は渡されない。したがってマルチキャストデータをアプリケーション 1 4 1 で正常に受信することができない。

## 【 0 0 1 0 】

また、暗号鍵を第 3 者に盗まれて解読されることを防ぐため、認証サーバ処理装置 1 0 1 は定期的に暗号鍵を生成し、ログイン時と同様に暗号鍵を受信者端末 1 3 0 へ配布する構成とすると良い。定期的に配布する暗号鍵をユーザ処理装置 1 3 2 が受け取らなかった場合は、既に受信者端末 1 3 0 がマルチキャスト通信を終了しているものとみなし、認証サーバ処理装置 1 0 1 にてログアウト処理を行う構成とすると、セキュリティの確保が図れる。

## 【 0 0 1 1 】

また、受信者端末 1 3 0 のアプリケーション 1 3 1 でマルチキャスト通信を終了すると、ユーザ処理装置 1 3 2 が認証サーバ処理装置 1 0 1 に対してログアウト要求を行い、認証サーバ処理装置 1 0 1 は該当ユーザの管理を終了する。

## 【 0 0 1 2 】

このようにして、認証サーバ処理装置 1 0 1 にはログイン・ログアウト処理によるユーザの認証履歴、定期的な暗号鍵の再送によるユーザの参加履歴が保存されるので、該当するマルチキャスト・グループの現在の参加者・参加人数を確定することができる。さらに、マルチキャストアドレスへのすべてのアクセスが履歴として残るので、不正なアクセス（未登録のユーザによるログインや同一ユーザの重複ログインなど）を発見することが可能になるセキュリティシステムである。なお、マルチキャストシステムはサブネットワーク 1 2 0 が複数あっても、無くても稼動する。

## 【 0 0 1 3 】

本発明の認証サーバ端末は、マルチキャストデータを送信する送信者端末に設けられた第 1 のユーザ処理装置からのログイン要求を受理する手段と、マルチキ

キャストデータを受信する送信者端末に設けられた第2のユーザ処理装置からのログイン要求を受理する手段と、送信者端末を有するユーザの個人情報が登録されたユーザ登録情報手段とを備える認証サーバ端末であって、前記認証サーバ処理装置からログインを許可された送信者端末はマルチキャストデータを暗号化して送信し、前記認証サーバ処理装置から予めユーザ登録情報手段にユーザとして登録された受信者端末は、ログインを許可されると共にマルチキャストデータを受信することを特徴とする構成としている。

## 【0014】

本発明のマルチキャスト受信者端末管理方法は、送信者端末を有するユーザの個人情報を登録し、マルチキャストデータを送信する送信者端末からのログイン要求を受理し、ログインを許可された送信者端末はマルチキャストデータを暗号化して送信し、マルチキャストデータを受信する送信者端末からのログイン要求を受理し、前記認証サーバ処理装置から予めユーザ登録情報手段にユーザとして登録された受信者端末は、ログインを許可されると共にマルチキャストデータを受信する手順としている。なお、送信者端末を有するユーザの個人情報を登録するのと同様にして、受信者端末を有するユーザの個人情報を登録しても良い。送信者端末に受信機能を設け、受信者端末に送信機能を設けると、認証サーバでの認証方法は同じなので、送信者端末でもデータ受信可能であるし、受信者端末からデータ送信可能となる。

## 【0015】

## 【発明の実施の形態】

以下、図面を用いて本発明の実施の形態を説明する。

図1を参照すると、本発明のマルチキャストにおける参加者管理セキュリティシステムの一実施例は、認証サーバ端末100と、送信者端末110、受信者端末130・140、インターネット/イントラネットなどのサブネットワーク120とから構成される。

## 【0016】

認証サーバ端末100の構成の詳細としては、ネットワークからの入力手段200と、ネットワークへの出力手段210、ユーザ認証処理手段220、鍵管理

手段 2 3 0、サーバ登録情報 2 4 0、サーバ管理情報 2 5 0 とから構成される（図 2）。送信者端末 1 1 0 の構成の詳細としては、ネットワークからの入力手段 3 0 0 と、ネットワークへの出力手段 3 1 0、入力データ処理手段 3 2 0、データ暗号処理手段 3 3 0、ユーザ登録情報 3 4 0、鍵情報 3 5 0、マルチキャスト通信可能なアプリケーション 1 1 1 とから構成される（図 3）。受信者端末 1 3 0・1 4 0 の構成の詳細としては、ネットワークからの入力手段 4 0 0 と、ネットワークへの出力手段 4 1 0、入力データ処理手段 4 2 0、データ復号処理手段 4 3 0、ユーザ登録情報 4 4 0、鍵情報 4 5 0、マルチキャスト通信可能なアプリケーション 1 3 1 とから構成される（図 4）。

## 【 0 0 1 7 】

ユーザ認証処理手段 2 2 0 は、ユーザ情報検索部 2 2 1 とユーザ認証部 2 2 2 を含む。鍵管理手段 2 3 0 は鍵更新制御部 2 3 1 と鍵生成部 2 3 2 を含む。入力データ処理手段 3 2 0 はデータ判別部 3 2 1 とユーザ情報作成部 3 2 2 を含む。データ暗号処理手段 3 3 0 は鍵管理部 3 3 1 と暗号データ作成部 3 3 2 を含む。入力データ処理手段 4 2 0 はデータ判別部 4 2 1 とユーザ情報作成部 4 2 2 を含む。データ暗号処理手段 4 3 0 は鍵管理部 4 3 1 と復号データ作成部 4 3 2 を含む。

## 【 0 0 1 8 】

これらの手段はそれぞれ概略つぎのように動作する。

サーバ登録情報 2 4 0 には、マルチキャスト通信する番組情報（マルチキャストアドレスやポート番号、暗号鍵の更新時間など）と番組の送受信を許可するユーザの情報（ユーザ ID やユーザの公開鍵など）をあらかじめ登録する。番組とはマルチキャストによる放送や会議の主催者により定められたマルチキャストアドレスとポート番号を使用し、主催者により定められたマルチキャストデータ送信開始時間から送信終了時間までのマルチキャストデータ通信を指す。また、ユーザ登録情報 3 4 0・4 4 0 には、ユーザの個人情報（ユーザ ID や参加予定の番組 ID、認証サーバ ID など）をあらかじめ登録する。

## 【 0 0 1 9 】

認証サーバ処理装置 1 0 1 において、入力手段 2 0 0 はユーザからのログイン

・ログアウト要求や暗号鍵の受理確認（ACK）を受信し、出力手段210はユーザ認証処理手段220による認証結果や鍵管理手段230によって生成された暗号鍵を送信するための通信装置である。ログアウト要求を受けたサーバ認証処理装置101は暗号鍵の更新・再送を中止し、ユーザの管理を終了する。この一連のユーザ管理情報をサーバ管理情報250へ書き込む。

#### 【0020】

次に送信者端末110において、アプリケーション111から受け取ったマルチキャストデータと入力手段300で受信した暗号鍵を入力データ処理手段320によって判別し、出力手段310はユーザ情報作成部322で作成したログイン・ログアウト要求情報やデータ暗号処理手段330による受理確認、暗号化したマルチキャストデータを送信する。

#### 【0021】

受信者端末130・140において、入力手段400から受け取ったマルチキャストデータと暗号鍵を入力データ処理手段420によって判別し、出力手段410はユーザ情報作成部422で作成したログイン・ログアウト要求情報やデータ復号処理手段430による受理確認を送信する。復号データ作成部432によって復号化されたマルチキャストデータをアプリケーション131で表示する。

#### 【0022】

このように構成された装置の動作を次に説明する。次に、図2の構成図のフローチャート図5、図3・図4の構成図のフローチャート図6を参照して本実施例の全体の動作について詳細に説明する。

認証サーバにおいては、まずユーザの秘密鍵によるデジタル署名を用いて暗号化されたログイン要求情報を受け取ることからユーザ（参加者）の管理が始まる。ユーザのフローについては後述する。ログイン要求情報はユーザID、番組IDのほかにタイムスタンプを含む（図5のステップA1）。ユーザ情報検索部221で、サーバ登録情報240に登録されているユーザIDから該当するユーザの公開鍵を検索しログイン要求情報を復号する。参加希望の番組に対してユーザIDが登録されているか確認する（ステップA2）。登録済みであれば認証し、認証結果をサーバ管理情報250に格納する。登録されていなければログインの

拒否を暗号化してユーザに通知し、この結果もサーバ管理情報 2 5 0 に格納する（ステップ A 3）。次に、鍵生成部 2 3 2 でサーバの秘密鍵でデジタル署名をした共通鍵をユーザの公開鍵で暗号化して送信し、次いでその共通鍵で暗号化した暗号鍵を送信する（ステップ A 4）。鍵の受理確認を受けた鍵更新制御部 2 3 1 はその結果をサーバ管理情報 2 5 0 に格納する。

## 【 0 0 2 3 】

待っても受理確認がこない場合は受信を終了したものとみなし、ログアウト処理しその情報をサーバ管理情報 2 5 0 に格納する。（ステップ A 5）。さらに、暗号鍵を不正に入手し利用されることを防ぐため、鍵更新制御部 2 3 1 において認証時刻から定期的に暗号鍵の再送を促す。番組が継続する場合は更新した暗号鍵をユーザへ配布する。番組が終了すると暗号鍵の配布も終了する（ステップ A 6）。また、ユーザからログアウト要求を受け取った場合は、該当ユーザへの更新した暗号鍵の配布を終了しログアウト処理を行い、その結果を暗号化してユーザへ送る。この結果はサーバ管理情報 2 5 0 に格納される（ステップ A 1）。

## 【 0 0 2 4 】

送信者がアプリケーション 1 1 1 を使ってマルチキャストデータを送信すると、まずデータ判別部 3 2 1 でそのマルチキャスト通信が認証サーバによる認証処理が済んでいるか確認する（図 6 のステップ B 1）。認証処理がされていない場合はユーザ登録情報 3 4 0 からユーザ ID、番組 ID（マルチキャストアドレスとポート番号）、認証サーバ ID（アドレスとポート番号）を取得しユーザ情報作成部 3 2 2 でログイン要求情報を作成し、事前に登録されていた認証サーバへ送信する（ステップ B 2）。認証結果を受け取り該当するマルチキャスト・グループへの通信を許可されると暗号化された暗号鍵を受け取る。認証されなかった場合はマルチキャストデータの送信を終了する（ステップ B 3）。暗号鍵は共通鍵暗号方式を用いて第 3 者による不正を保護している。復号するためには、ログイン後にサーバの秘密鍵によるデジタル署名を施した共通鍵を取得し、デジタル署名が正しい認証サーバのものであることを確認し、鍵管理部 3 3 1 で鍵情報 3 5 0 に管理する。

## 【 0 0 2 5 】

その後、配布された暗号鍵を保管している共通鍵で復号化し受理確認を認証サーバへ送信する（ステップB4）。暗号データ作成部332においてその暗号鍵を用いてマルチキャストデータを暗号化し暗号鍵のIDを付加して送信する（ステップB5）。認証後、継続してマルチキャストデータを送信する際、認証サーバから更新された暗号鍵を受信したら受理確認を送信する。更新された暗号鍵がなければ既存の暗号鍵を用いて暗号化する（ステップB6）。上記のフローをマルチキャストデータが継続するまで繰り返し、データ判別部321がアプリケーション111から送信終了の要求を受けると、ユーザ登録情報340からユーザID、番組ID（マルチキャストアドレスとポート番号）、認証サーバID（アドレスとポート番号）を取得し、ユーザ情報作成部322でログアウト要求情報を作成し認証サーバへ送信してマルチキャスト通信を終了する（ステップB7）。

#### 【0026】

受信者のフローは基本的に送信者と同形である。マルチキャストデータを受信すると、まずデータ判別部421でそのマルチキャスト通信が認証サーバによる認証処理が済んでいるか確認する（図6のステップB1）。認証処理がされていなければユーザ登録情報440からユーザID、番組ID（マルチキャストアドレスとポート番号）、認証サーバID（アドレスとポート番号）を取得しユーザ情報作成部422でログイン要求情報を作成し、事前に登録されていた認証サーバへ送信する（ステップB2）。認証結果を受け取り該当するマルチキャスト・グループへの通信を許可されると暗号化された暗号鍵を受け取る。認証されなかった場合はマルチキャストデータの受信を終了する（ステップB3）。暗号鍵は共通鍵暗号方式を用いて第3者による不正を保護している。復号するためには、ログイン後にサーバの秘密鍵によるデジタル署名を施した共通鍵を取得し、デジタル署名が正しい認証サーバのものであることを確認し、鍵管理部431により鍵情報450に管理する。

#### 【0027】

その後、保管している共通鍵で配布された暗号鍵を復号化し受理確認を認証サーバへ送信する（ステップB4）。復号データ作成部432において暗号鍵ID

から該当する暗号鍵を検索し、その暗号鍵でマルチキャストデータを復号化してアプリケーション 1 3 1 で受信する（ステップ B 5）。認証後、継続してマルチキャストデータを受信する際、認証サーバから更新された暗号鍵を受信したら受理確認を送信する。更新された暗号鍵がなければ既存の暗号鍵を用いて復号化する（ステップ B 6）。上記のフローをマルチキャストデータが継続するまで繰り返し、データ判別部 4 2 1 がアプリケーション 1 3 1 から受信終了の要求を受けると、ユーザ登録情報 4 4 0 からユーザ ID、番組 ID（マルチキャストアドレスとポート番号）、認証サーバ ID（アドレスとポート番号）を取得し、ユーザ情報作成部 4 2 2 でログアウト要求情報を作成し認証サーバへ送信してマルチキャスト通信を終了する（ステップ B 7）。

## 【 0 0 2 8 】

次に、本発明の他の実施例について説明する。先の実施例において送信者が認証サーバを管理することができる場合、送信者端末上で認証サーバを実施する形態を設けることで、端末構成を簡素化でき、送信者用の暗号鍵をネットワーク上に流すことなく管理できるようになる。

図 7 を参照すると、本実施例は、認証サーバ兼送信者端末 5 0 0、受信者端末 5 1 0、インターネット/イントラネットなどのサブネットワーク 5 2 0 とから構成される。認証サーバ兼送信者端末 5 0 0 は認証サーバ処理装置 5 0 1、マルチキャスト対応アプリケーション 5 0 2、ユーザ処理装置 5 0 3 とから構成されている。受信者端末 5 1 0 はマルチキャスト対応アプリケーション 5 1 1、ユーザ処理装置 5 1 2 とから構成されている。

## 【 0 0 2 9 】

認証サーバ兼送信者端末 5 0 0 は前述した図 2 と図 3 を組み合わせた装置を有し、受信者端末 5 1 0 は図 4 と同一の装置を有する。本実施例におけるこれらの装置の動作の違いは、入力手段 2 0 0・3 0 0 及び出力手段 2 1 0・3 1 0 はネットワークとの通信装置であったことに対し、出力手段 2 1 0 の出力先が入力手段 3 0 0 となり、ユーザ情報作成部 3 2 2 及び鍵管理部 3 3 1 による出力手段 3 1 0 の出力先が入力手段 2 0 0 となるという点である。

## 【 0 0 3 0 】

本実施例の全体の動作については、認証サーバ兼送信者端末 5 0 0 は前述した図 5・図 6 の処理を並列に行い、受信者端末 5 1 0 は図 6 と同一の処理を行う。

【 0 0 3 1 】

【発明の効果】

以上説明したように、本発明によれば、第 1 の効果は、現在誰がマルチキャスト・グループに参加しているかを確定できることにある。認証サーバにおいて、ユーザ ID により各ユーザのログイン・ログアウト状況が管理されるため、送信者は受信してほしいユーザが存在していることを知ることができ、そのユーザの受信状況（受信開時間や受信終了時間）も知ることができるので、ユーザ管理に有効である。

【 0 0 3 2 】

第 2 の効果は、第 3 者の不正を防ぐことができることにある。重要なデータを流している場合は、そのデータが第 3 者に漏洩してしまうことを防ぐ必要がある。マルチキャストシステムはマルチキャスト・グループにアクセスしたすべてのユーザ情報が管理されるため、第 3 者の侵入にいち早く気づき対処することができる。

【図面の簡単な説明】

【図 1】 本発明の一実施の形態を説明する構成ブロック図である。

【図 2】 認証サーバ端末の詳細な構成ブロック図である。

【図 3】 送信者端末の詳細な構成ブロック図である。

【図 4】 受信者端末の詳細な構成ブロック図である。

【図 5】 認証サーバ端末の動作を説明するフローチャートである。

【図 6】 送信者端末並びに受信者端末の動作を説明するフローチャートである。

【図 7】 本発明の第 2 の実施の形態を説明する構成ブロック図である。

【符号の説明】

1 0 0 認証サーバ端末

1 0 1 認証サーバ処理装置

1 1 0 送信者端末



1 2 0 サブネットワーク

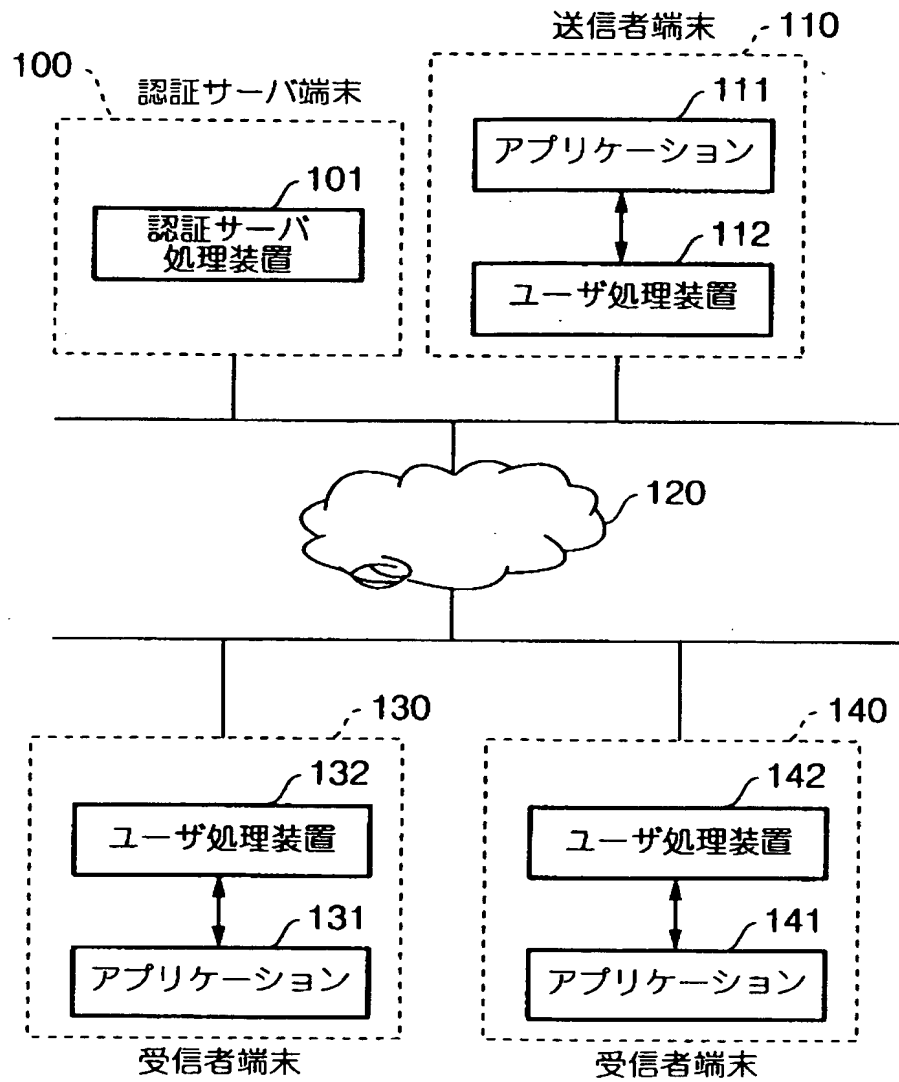
1 3 0 受信者端末

1 4 0 受信者端末

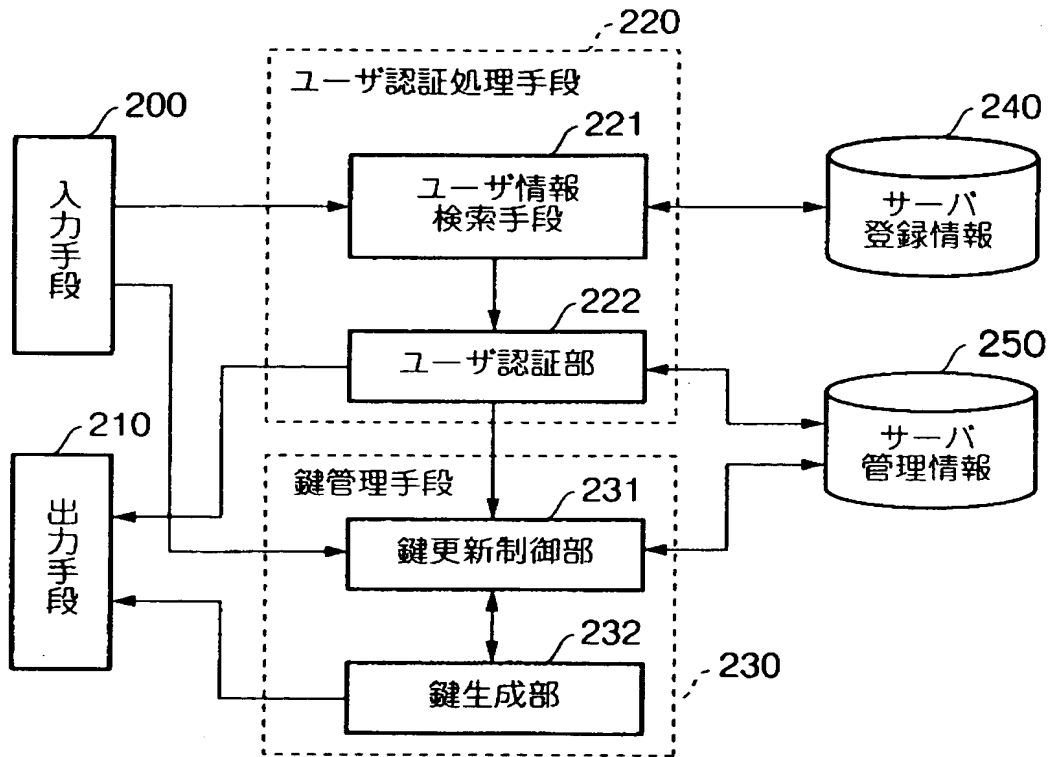
【書類名】

図面

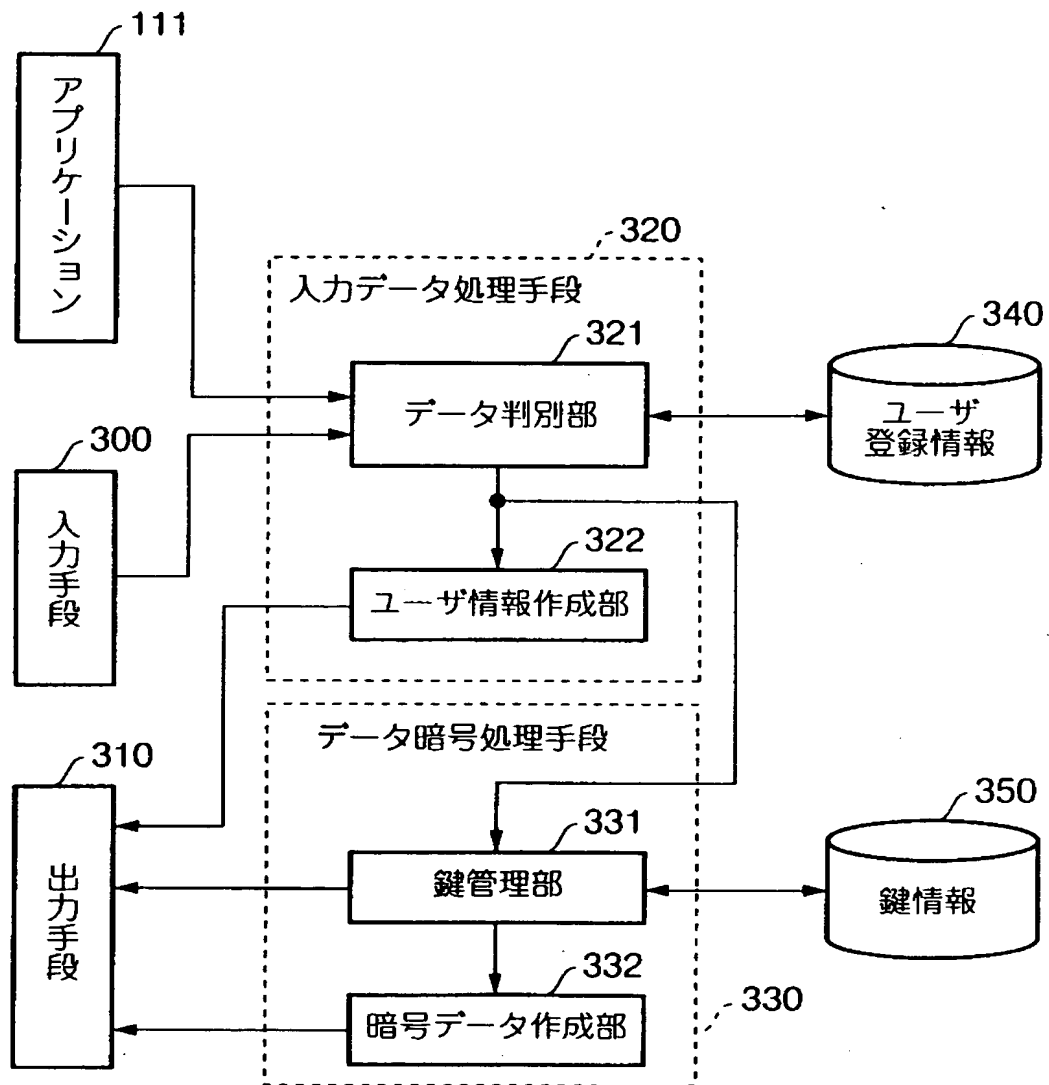
【図 1】



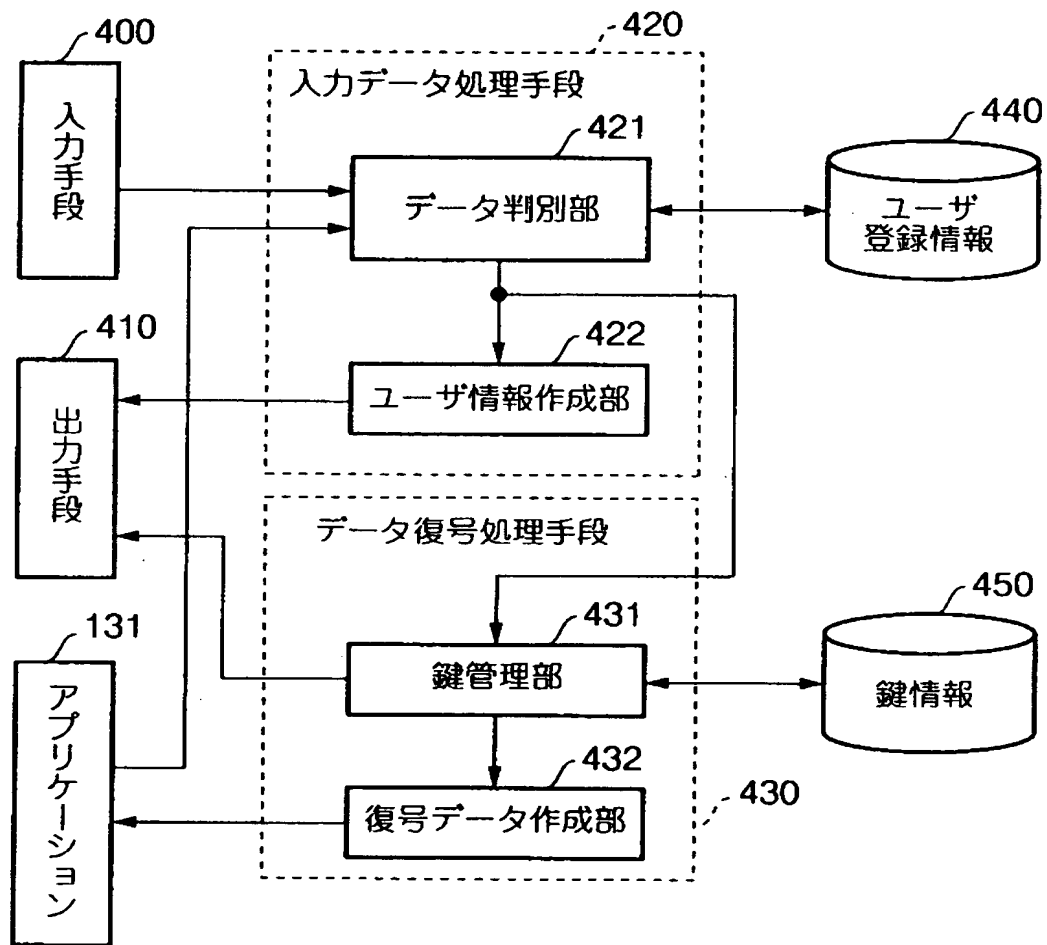
【図 2】



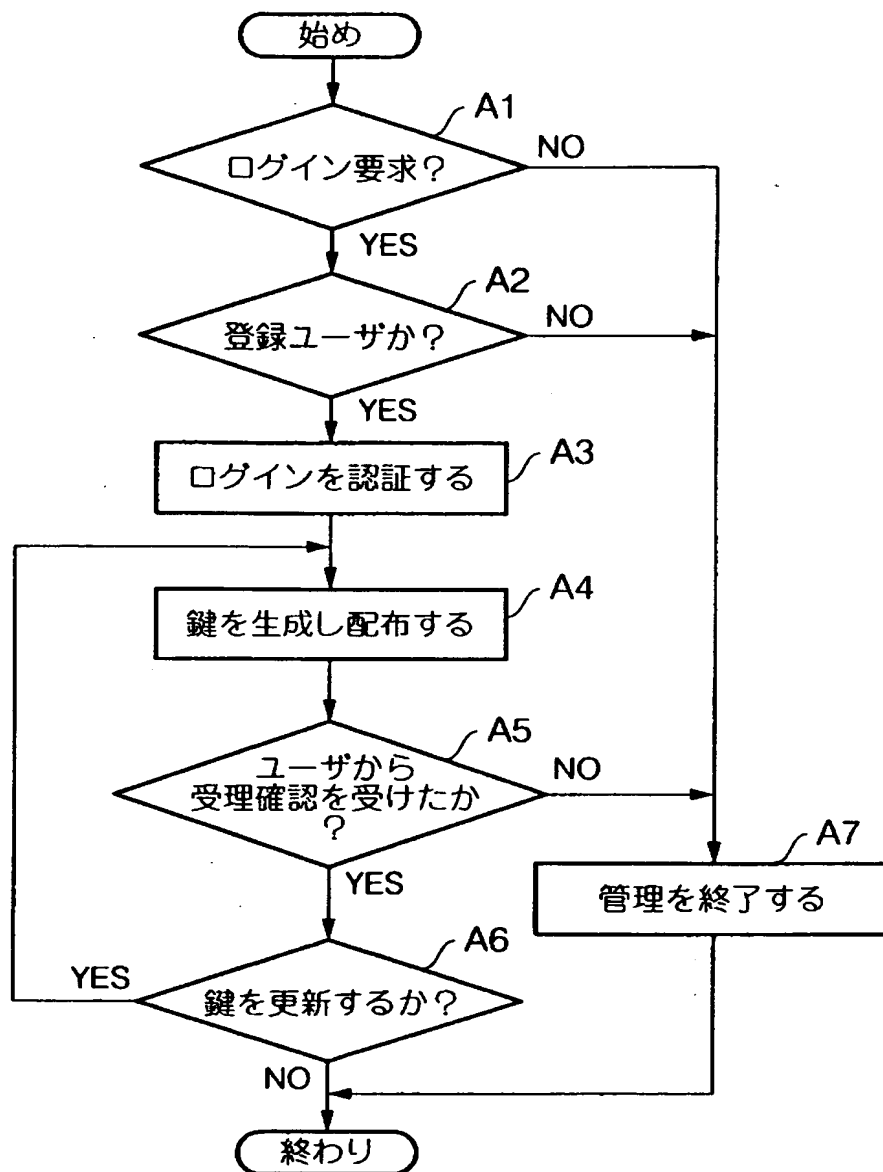
【図 3】



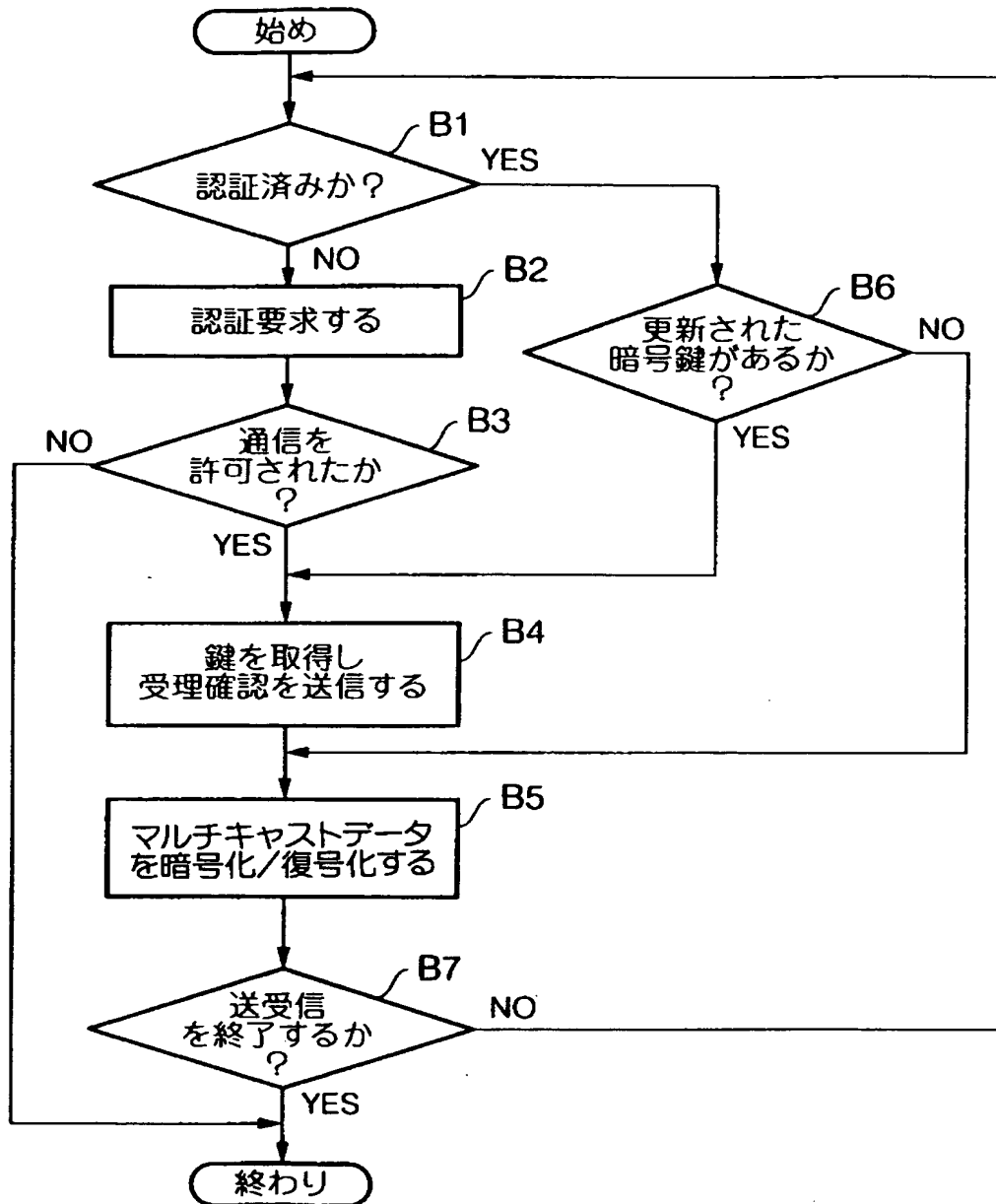
【図 4】



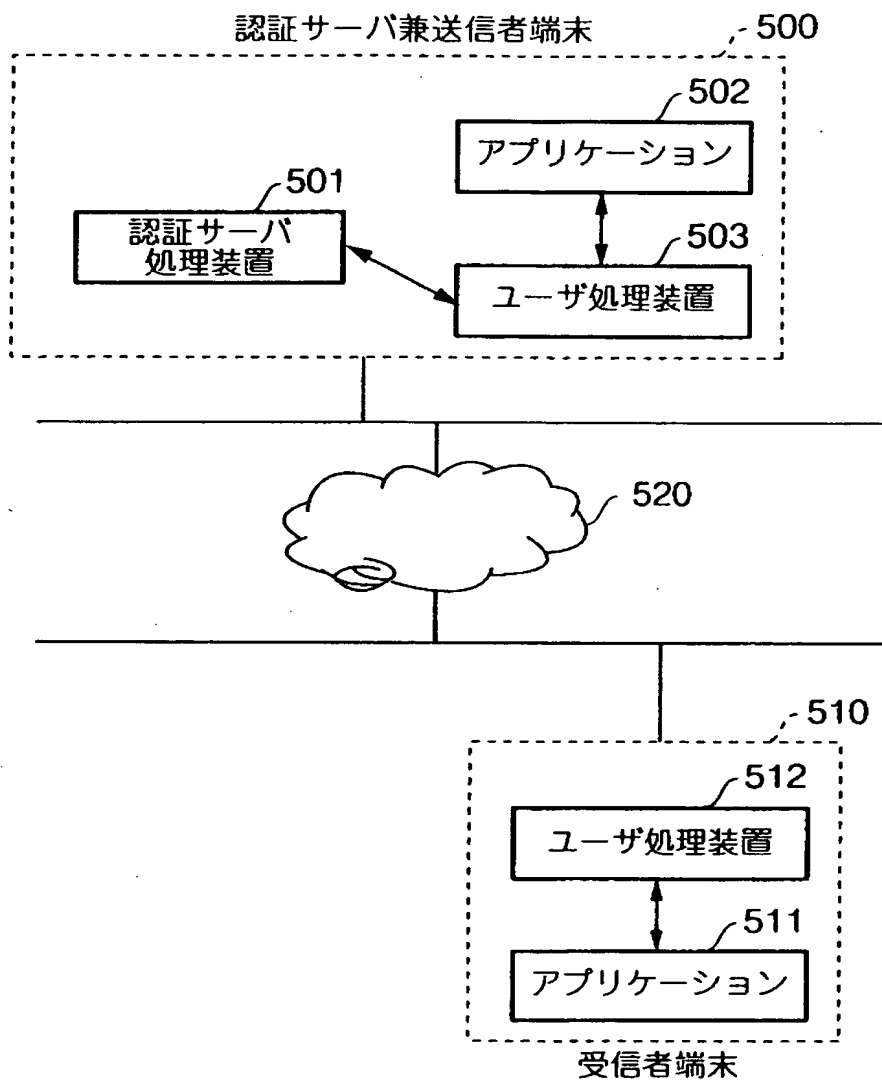
【図 5】



【図 6】



【図 7】





【書類名】 要約書

【要約】

【課題】 マルチキャストによるデータ通信において、指定された認証サーバで参加者を個別認証することにより参加者を特定できるマルチキャストシステムを提供する。

【解決手段】 本発明のマルチキャストシステムは、マルチキャストにおける送信者端末 1 1 0 と受信者端末 1 3 0、1 4 0 の管理を行う認証サーバ処理装置 1 0 1 と、該認証サーバ処理装置に対するログインを行う第 1 のユーザ処理装置 1 1 2 を有し、マルチキャストデータを送信する送信者端末 1 1 0 と、該認証サーバ処理装置に対するログインを行う第 2 のユーザ処理装置 1 3 2 を有し、マルチキャストデータを受信する受信者端末 1 3 0 とを備えるものである。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2000-073064
受付番号	50000312834
書類名	特許願
担当官	濱谷 よし子 1614
作成日	平成 12 年 3 月 23 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000004237
【住所又は居所】	東京都港区芝五丁目 7 番 1 号
【氏名又は名称】	日本電気株式会社

【代理人】

申請人

【識別番号】	100108578
【住所又は居所】	東京都新宿区高田馬場 3 丁目 23 番 3 号 ORビ ル 志賀国際特許事務所

【氏名又は名称】	高橋 詔男
----------	-------

【代理人】

【識別番号】	100064908
【住所又は居所】	東京都新宿区高田馬場 3 丁目 23 番 3 号 ORビ ル 志賀国際特許事務所

【氏名又は名称】	志賀 正武
----------	-------

【選任した代理人】

【識別番号】	100101465
【住所又は居所】	東京都新宿区高田馬場 3 丁目 23 番 3 号 ORビ ル 志賀国際特許事務所

【氏名又は名称】	青山 正和
----------	-------

【選任した代理人】

【識別番号】	100108453
【住所又は居所】	東京都新宿区高田馬場 3 丁目 23 番 3 号 ORビ ル 志賀国際特許事務所

【氏名又は名称】	村山 靖彦
----------	-------

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日	1990年 8月29日
[変更理由]	新規登録
住 所	東京都港区芝五丁目7番1号
氏 名	日本電気株式会社